CLAIMS

What is claimed:

1. A method comprising the computer implemented steps of:

sorting a plurality of data items belonging to a superset of data items;

deriving a plurality of ranges using adjacent pairs of data items in said sorted plurality of data items as endpoints such that all data items in said plurality of the data items are at endpoints of said plurality of ranges and such that all other data items in said superset fall in-between the endpoints of said plurality of ranges;

generating a hash tree having leaf nodes that represent the plurality of ranges;

digitally signing a root node of the tree; and

electronically transmitting said digitally signed root node and parts of said tree onto a network for use in cryptographically demonstrating whether a given data item is one of said plurality of data items.

2. The method of claim 1, wherein said step of generating said tree includes the step of:

forming leaf nodes from endpoints of said plurality of ranges.

3. The method of claim 2, wherein said step of generating said tree includes the step of:

forming an adjacent pair of leaf nodes from different endpoints of one of said plurality of ranges.

4. The method of claim 1, wherein said step of generating said tree includes the step of:

forming each of a plurality of the leaf nodes from the endpoints of a different one of said plurality of ranges.

5. The method of claim 1, wherein said plurality of data items identify digital certificates sharing an attribute.

6. The method of claim 5, wherein said attribute is that the digital certificates are revoked.

7. The method of claim 1, wherein said plurality of data items identify digital signatures.

8. The method of claim 1, wherein said plurality of data items identify digital signatures on binary code.

9. The method of claim 1, wherein said plurality of data items identify revoked credit cards.

10. A method comprising the computer implemented steps of:

receiving a request message requesting whether a first data item is one of a plurality of data items belonging to a superset of data items;

selecting a range that is derived from ~~the~~ a pair of data items in said plurality of data items that defines the smallest range that includes said first data item, wherein the first data item is not one of the plurality of data items if the first data item is in-between the endpoints of the selected range, and wherein the first data item is one of said plurality of data items if said first data item is on one of the endpoints of the selected range;

determining, for a tree having leaf nodes that represent ranges derived from adjacent pairs of said plurality of data items in a sorted list of said plurality of data items, a path through said tree from said selected range to a first of a set of root nodes; and

generating a response message that includes,

data identifying said selected range in said response message,

a set of nodes in said tree such that each node in said set of nodes and at least a previously identified node on said path can be combined to identify a previously unidentified node on said path, until said first root node is identified,

the set of nodes and excluding at least certain nodes on the path from the response message, and

a digitally signed representation of the first root node in said response message; and

electronically transmitting the response message onto a network.

11. The method of claim 10, wherein the endpoints of the selected range are independently hashed and then hashed together to generate a node in the tree.

12. The method of claim 10, wherein each leaf node specifies one of one range, an endpoint of one range, a hashed range, and a hashed endpoint of one range.

13. The method of claim 10, wherein said plurality of data items identify digital certificates sharing an attribute.

14. The method of claim 13, wherein said attribute is that the digital certificates are revoked.

15. The method of claim 10, wherein said plurality of data items identify digital signatures.

16. The method of claim 10, wherein said plurality of data items identify digital signatures on binary code.

17. The method of claim 10, wherein said plurality of data items identify revoked credit cards.

18. A method comprising the computer implemented steps of:

electronically transmitting a request message as to whether a first data item is one of a plurality of data items belonging to a superset of data items;

receiving a response message that includes,

a digitally signed representation submitted to be a root node of a tree having leaf nodes that represent ranges, the ranges derived from adjacent pairs of data items in a sorted list of said plurality of data items,

data identifying the range that includes said first data item, and

a set of nodes in said tree sufficient to generate said root node starting from said range; and

determining if said first data item is one of said plurality of data items based on said range, wherein the first data item is not one of the plurality of data items if the first data item is in-between the endpoints of the selected range, and wherein the first data item is one of said plurality of data items if said first data item is on one of the endpoints of the selected range; and

generating said root node using said range and the set of nodes; and

determining if said digitally signed representation matches said root node.

19. The method of claim 18, wherein said set of nodes includes nodes that together with a node on a path from the range to the root node can be used to generate a next node on the path, but excluding at least some nodes that are on the path.

20. The method of claim 18, wherein said step of receiving the response message includes the step of:

generating a node in said tree from the range that includes the first data item and another range identified in said response message.

21. The method of claim 18, wherein each node in said set of nodes and at least a previously identified node on a path from the range to the root node can be combined to identify a previously unidentified node on said path, until said root node is identified.

22. The method of claim 18, wherein each leaf node specifies one of one range, an endpoint of one range, a hashed range, and a hashed endpoint of one range.

23. The method of claim 18, wherein said plurality of data items identify digital certificates sharing a attribute.

24. The method of claim 23, wherein said attribute is that the digital certificates are revoked.

25. The method of claim 18, wherein said plurality of data items identify digital signatures.

26. The method of claim 18, wherein said plurality of data items identify digital signatures on binary code.

27. The method of claim 18, wherein said plurality of data items identify revoked credit cards.